

(Translation of the front page  
of the priority document of  
Japanese Patent Application  
No. 2001-161403)

PATENT OFFICE  
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of  
the following application as filed with this Office.

Date of Application : April 23, 2001  
Application Number : Patent Application  
2001-161403  
Applicant(s) : Humming Heads Inc.

November 9, 2001

Commissioner,  
Japan Patent Office

Kouzo Oikawa

Certification Number 2001-3098288

日 本 国 特 許 庁  
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日  
Date of Application:

2001年 4月23日

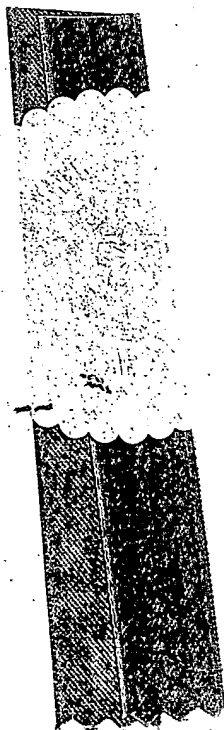
出 願 番 号  
Application Number:

特願2001-161403

出 願 人  
Applicant(s):

ハミングヘッズ株式会社

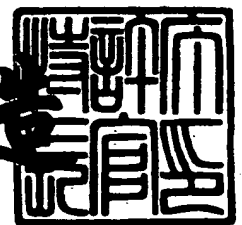
CERTIFIED COPY OF  
PRIORITY DOCUMENT



2001年11月 9日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3098288

【書類名】 特許願  
【整理番号】 HH08PH1301  
【提出日】 平成13年 4月23日  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 17/00  
【発明者】

【住所又は居所】 東京都中央区月島一丁目2番13号 ハミングヘッズ  
株式会社内

【氏名】 大江 尚之

【発明者】

【住所又は居所】 東京都中央区月島一丁目2番13号 ハミングヘッズ  
株式会社内

【氏名】 志摩 貴浩

【特許出願人】

【識別番号】 500083226

【住所又は居所】 東京都中央区月島一丁目2番13号

【氏名又は名称】 ハミングヘッズ株式会社

【代表者】 大江 尚之

【電話番号】 03-3531-7281

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【先の出願に基づく優先権主張】

【出願番号】 特願2000-352113

【出願日】 平成12年11月20日

【書類名】 明細書

【発明の名称】 コンピュータリソースの制御方法および装置並びに記録媒体

【特許請求の範囲】

【請求項1】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御する方法であって、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第1のステップと、

前記第1のステップで捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第2のステップと、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第3のステップと、

アクセス権限がなければ当該操作要求を拒否する第4のステップとを備えることを特徴とするコンピュータリソースの制御方法。

【請求項2】 前記第1のステップに代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第5のステップを備えることを特徴とする請求項1に記載のコンピュータリソースの制御方法。

【請求項3】 前記第2のステップが、

特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定するステップまたは、

コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定するステップまたは、

アクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定するステップ

を備えることを特徴とする請求項 1 または 2 に記載のコンピュータリソースの制御方法。

【請求項 4】 前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも 1 つを指定する情報を含むことを特徴とする請求項 3 に記載のコンピュータリソースの制御方法。

【請求項 5】 前記第 4 のステップは、

要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返すステップから成ることを特徴とする請求項 1 ～ 4 のいずれか一項に記載のコンピュータリソースの制御方法。

【請求項 6】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御するリソース制御手段を備えたコンピュータ装置であって、

前記リソース制御手段が、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 1 の手段と、

前記第 1 の手段で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第 2 の手段と、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第 3 の手段と、

アクセス権限がなければ当該操作要求を拒否する第 4 の手段とを備えることを特徴とするコンピュータ装置。

【請求項 7】 前記第 1 の手段に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 5 の手段を備えることを特徴とする請求項 6 に

記載のコンピュータ装置。

【請求項 8】 前記第 2 の手段が、

特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定する手段または、

コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定する手段または、

アクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定する手段

を備えることを特徴とする請求項 6 または 7 に記載のコンピュータ装置。

【請求項 9】 前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも 1 つを指定する情報を含むことを特徴とする請求項 8 に記載のコンピュータ装置。

【請求項 10】 前記第 4 の手段は、

要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す手段から成ることを特徴とする請求項 6 ～ 9 のいずれか一項に記載のコンピュータ装置。

【請求項 11】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを制御するリソース制御プログラムを記録した媒体であって、

前記リソース制御プログラムが、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 1 の処理

と、

前記第 1 の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第 2 の処理と、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第 3 の処理と、

アクセス権限がなければ当該操作要求を拒否する第 4 の処理とを備えることを特徴とするコンピュータが読取り可能なプログラムを記録した記録媒体。

【請求項 1 2】 前記第 1 の処理に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 5 の処理を備えることを特徴とする請求項 1 に記載の記録媒体。

【請求項 1 3】 前記第 2 の処理が、

特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定する処理または、

コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定する処理または、

アクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する処理

を備えることを特徴とする請求項 1 1 または 1 2 に記載の記録媒体。

【請求項 1 4】 前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも 1 つを指定する情報を含むことを特徴とする請求項 1 3 に記載の記録媒体。

【請求項 1 5】 前記第 4 の処理は、

要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知

を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理から成ることを特徴とする請求項 1 1 ～ 1 4 のいずれか一項に記載の記録媒体。

【請求項 1 6】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを制御するリソース制御プログラムであって、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 1 の処理と、

前記第 1 の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第 2 の処理と、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第 3 の処理と、

アクセス権限がなければ当該操作要求を拒否する第 4 の処理とを備えることを特徴とするコンピュータが実行可能なリソース制御プログラム。

【請求項 1 7】 前記第 1 の処理に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 5 の処理を備えることを特徴とする請求項 1 6 に記載のリソース制御プログラム。

【請求項 1 8】 前記記載の処理においてアクセス権限がないと判定され、アクセスを拒否された場合課金することによってアクセス権限を許可することを特徴とするリソース制御プログラム。

【請求項 1 9】 前記記載のコンピュータリソースとは、ウェブキャスト、デジタル放送、音楽配信等のコンテンツを含むことを特徴とするリソース制御プログラム。

【発明の詳細な説明】

【 0 0 0 1 】



【発明の属する技術分野】

本発明は、ファイル、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを管理するコンピュータリソースの制御方法および装置並びに記録媒体に関するものである。

【0002】

【従来の技術】

従来において、パーソナルコンピュータ等のコンピュータにおけるファイルや記憶装置等のリソースをアプリケーションプログラムを介してユーザがアクセスする場合に、アクセス権限のないユーザに情報が解読または盗聴されるのを防ぐために、オペレーティングシステム（以下、OS）内にアクセス権限のチェック機能を設ける方法、あるいは専用のアクセス管理ツールを付加してアクセス権限のチェックを行なう方法が知られている。

【0003】

例えばWindows（米国マイクロソフト社の登録商標）に代表される汎用のOSにおいては、ファイルの読取り、書き込み、実行をアクセス権限のないユーザに対しては許可しない機能が備わっている。また、ファイルの削除、アクセス権限の変更、所有権の変更についての権限を設定可能にした汎用OSもある。

また、アクセス管理ツールとして、例えば特開平7-84852公報に開示されているように、ファイルの参照と共に複写の可否を登録し、その可否によって参照、複写を制限するものが知られている。詳しくは、表示領域に読出し制限の属性を付加し、表示画面のハードコピーを防止するものが知られている。

【0004】

【発明が解決しようとする課題】

アクセス権限のないユーザに対して情報の持ち出しを全面的に禁止するためには、図9に示すように、メールへの添付、印刷、ファイル移動／ファイルコピー、クリップボードへのコピー、フロッピーディスクへの別名保存、オブジェクトの貼り付け、画面ハードコピーなどの機能を制限する必要がある。さらに、ネットワークを通じた情報の持ち出しを制限する必要がある。

しかしながら、上記従来技術にあつては、ファイル及び画面のハードコピー以

外の操作（例えばクリップボードへのコピー）に対して制限することができないという問題がある。もしも、クリップボードへのコピーなどの操作を制限しようとする場合には、OSまたはアプリケーション自体に変更を加えることが必要になり、汎用的な応用ができないという問題がある。

## 【0005】

本発明の目的は、OSやプロセス（OSの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限し、しかも既存環境における禁止または制限事項を拡張することができるコンピュータリソースの制御方法および装置並びに記録媒体を提供することにある。

## 【0006】

## 【課題を解決するための手段】

上記目的を達成するために、本発明のコンピュータリソースの制御方法は、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第1のステップと、前記第1のステップで捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第2のステップと、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第3のステップと、アクセス権限がなければ当該操作要求を拒否する第4のステップとを備えることを特徴とする。

また、前記第1のステップに代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第5のステップを備えることを特徴とする。

また、前記第2のステップが、特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを

参照し、アクセス権限があるか否かを判定するステップ、またはコンピュータリソース内部に記述された既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定するステップ、またはアクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定するステップを備えることを特徴とする。

また、前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも1つを指定する情報を含むことを特徴とする。

また、前記第4のステップは、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返すステップから成ることを特徴とする。

#### 【0007】

さらに、コンピュータリソースに対するアクセスを制御するリソース制御手段を備えた本発明に係るコンピュータ装置は、

前記リソース制御手段が、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第1の手段と、前記第1の手段で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第2の手段と、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第3の手段と、アクセス権限がなければ当該操作要求を拒否する第4の手段とを備えることを特徴とする。

また、前記第1の手段に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第5の手段を備えることを特徴とする。

また、前記第2の手段が、特定のコンピュータリソースを指定するリソース指

定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定する手段、またはコンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定する手段、またはアクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定する手段を備えることを特徴とする。

また、前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも1つを指定する情報を含むことを特徴とする。

また、前記第4の手段は、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す手段から成ることを特徴とする。

#### 【0008】

さらに本発明に係るリソース制御プログラムを記録した媒体は、前記リソース制御プログラムが、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第1の処理と、前記第1の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第2の処理と、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第3の処理と、アクセス権限がなければ当該操作要求を拒否する第4の処理とを備えることを特徴とする。

また、前記第1の処理に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第5の処理を備えること特徴とする。

また、前記第2の処理が、特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定する処理、またはコンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定する処理、またはアクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定する処理を備えることを特徴とする。

また、前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも1つを指定する情報を含むことを特徴とする。

また、前記第4の処理は、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理から成ることを特徴とする。

#### 【0009】

さらにコンピュータリソースに対するアクセスを制御する本発明に係るリソース制御プログラムは、前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第1の処理と、前記第1の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第2の処理と、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第3の処理と、アクセス権限がなければ当該操作要求を拒否する第4の処理とを備えることを特徴とする。

発明者は本装置をH. Hコンピュータセキュリティ方式と命名した。

#### 【0010】

#### 【発明の実施の形態】

【第 1 実施形態】

以下、本発明の実施の形態を図面により詳細に説明する。

図 1 (a), (b) は本発明を実施する環境の一実施の形態を示すハードウェア構成図である。

図 1 (a) に示す構成は、スタンドアロン構成におけるコンピュータ 1 0 1 のハード構成を示すものであり、ハードディスク (HDD) 1 0 1 1 を備えたパーソナルコンピュータ (PC) 1 0 1 2、ディスプレイ 1 0 1 3、プリンタ 1 0 1 4、外部にリソースデータを出力することが可能な外部装置 1 0 1 5 で構成されている。

パーソナルコンピュータ 1 0 1 2 には、汎用の OS とアプリケーションが組み込まれており、さらに本発明に係るリソース管理プログラムが組み込まれている。

図 1 (b) は、ネットワーク 1 0 2 を利用する場合の構成を示すものであり、図 1 (a) に示したのと同様な構成のコンピュータ 1 0 1 a ~ 1 0 1 c がネットワーク 1 0 2 で接続されている。

【0 0 1 1】

このような構成において、一般的に、アプリケーションが OS の管理するリソースにアクセスするには、OS が提供する API (Application Program Interface) を利用する。この API の利用方法は OS により確定しており、API を利用する実行コード部を判別することができる。本発明では、リソースへのアクセスに必要なすべての API を監視する監視ルーチンを設け、アプリケーションが API を利用する前に、その実行コード部を変更するか、API 処理の入りを監視ルーチンと置き換えることで、API 利用時に監視ルーチンが利用されるようにする。監視ルーチンは、アプリケーションが求める API を処理するか、もしくは API の処理をせずに不正命令としてアプリケーションに結果を返す。本発明のリソース管理プログラムによって拡張したアクセス権の管理は、OS の管理とは別に本プログラムが管理し、アクセス権の種類別に監視ルーチンを設ける。この方法により、リソースを不正に利用するアプリケーションから、そのアクセスを制限する。

## 【0012】

図2は、本発明に係るリソース管理プログラム203の構成及びAPI監視／制御の概念を示す図であり、リソース管理プログラム203はAPI監視コントローラ（API監視CTRL）2031、APL監視コントローラ（APL監視CTRL）2032、アクセス制御コントローラ（アクセス制御CTRL）2033、OS監視コントローラ（OS監視CTRL）2034から構成されており、リソースアクセス要求を出すアプリケーション2021や画面キャプチャなどのOS機能操作2022を備える一般的なアプリケーションからなるユーザ環境202と汎用OS201との間に位置し、汎用OS201およびユーザ環境202が提供するリソースに対する要求を監視するようになっている。

なお、汎用OS201は、OSが管理するリソース2011と、OSがアプリケーション2021に提供しているAPI群2012を備える。

## 【0013】

本発明に係るリソース管理プログラム203におけるAPI監視CTRL2031は、アクセス制御を行なうのに必要な全てのAPIを監視するモジュールである。また、APL監視CTRL2032は、アプリケーション2021が保持しているリソースを記憶するモジュールである。アクセス制御CTRL2033はアクセスが許可されているかを判断するモジュールであり、アクセス権管理テーブル2035を備える。また、OS監視CTRL2034は、汎用OS201の機能によってリソースへアクセスする操作を監視するモジュールである。

## 【0014】

アクセス権限テーブル2035は、図3に示すように、リソース指定情報20351、条件20352、n個のアクセス権情報20353～2035nをリソース毎に登録可能に構成されている。

リソース指定情報20351は、汎用OS201が管理しているリソースのうち、特定のものを指定するための情報であり、例えば、ファイルの場合はファイル名やファイルIDなどの情報が登録される。通信データの場合は、ホスト名、ポート番号、IPアドレスなどが登録され、メモリの場合は、そのオブジェクトを示すオブジェクト名、アドレスなどが登録される。また、外部出力装置の場合

は、そのデバイスドライバを示すデバイス名などが登録される。

条件 2 0 3 5 2 は、アクセス権が有効となる条件またはその組み合わせをしめすものであり、例えばユーザ名 / I D , グループ名 / I D , 時刻, 使用アプリケーションなどが登録される。

アクセス権情報 2 0 3 5 3 ~ 2 0 3 5 n は、既存環境で定義されていない拡張したアクセス権のうち、指定したリソースに付加した権限を示すものであり、例えば他媒体への移動権限, 他媒体へのコピー権限, 印刷権限, 共有メモリへの読み込み権限 ( W i n d o w s ではクリップボードなど) , 画面ハードコピー権限, 使用アプリケーションの限定 ( 特定アプリケーション以外での使用禁止やメール添付の禁止) などが登録される。

なお、一般的に、リソースへのアクセスは複数の A P I によって行われることがあり、その場合はリソース指定情報は O S が管理する I D ( ハンドルなど) に変換されることがある。その場合、リソース管理プログラム 2 0 3 の内部においては、リソース指定情報とその I D は同一視するようにしている。

#### 【 0 0 1 5 】

このような構成に係るリソース管理プログラム 2 0 3 の処理について、図 2 の ① ~ ⑨ で示す情報伝達手順に従って説明する。

①アプリケーション 2 0 2 1 からリソースへのアクセス要求があれば、 A P I 監視 C T R L 2 0 3 1 がその要求を捕捉し、アクセス制御 C T R L 2 0 3 3 に伝える。

②アクセス制御 C T R L 2 0 3 3 は、アクセス権限チェックを行なう際、必要に応じて、アプリケーション 2 0 2 1 が保持しているリソースの情報を A P L 監視 C T R L 2 0 3 2 から取得する。

③アクセスを拒否する条件として 2 通りあるが、第 1 の条件 A ( アクセス拒否 A ) では、上記 ① のアクセス要求に対してアクセス権限チェックを行なう。権限がない場合、アプリケーション 2 0 2 1 が発行した A P I の処理を行わずに、結果としてアクセス違反のエラーを返す。

④第 2 の条件 B ( アクセス拒否 B ) では、②のアクセス要求に対してアクセス権限チェックを行なう。権限がなく、かつ、アプリケーション 2 0 2 1 が発行し



たAPIの結果としてエラーを返すことができない場合、アプリケーション2021が要求したリソースへの処理を行わずに、リソース管理プログラム203が予め用意したダミーのリソースへのアクセス要求に代えて、APIの処理を行なう。

その結果、アプリケーション2021は要求に成功したように動作するが、実際には要求したリソースにアクセスできない。

【0016】

⑤アクセス要求①に対してアクセス権限チェックを行った結果、権限がある場合、API監視CTRL2031がその要求を捕捉し、アプリケーション2021が発行したAPIの処理をそのまま汎用OS201に伝え、その結果をアプリケーション2021に返す。

⑥上記⑤の処理によって、APIが成功し、かつ、そのAPIによってアプリケーション2021がリソースを保持する場合は、APL監視CTRL2032に伝える。APL監視CTRL2032はアプリケーション2021と保持しているリソースの対応を登録する。

アプリケーション2021がリソースの解放要求APIを発行し、かつそのAPIが成功した場合も、APL監視CTRL2032に伝える。APL監視CTRL2032はアプリケーション2021と保持していたリソースの対応を抹消する。

⑦OS標準機能の操作によって、リソースへのアクセス要求があれば、OS監視CTRL2034がその要求を捕捉し、アクセス制御CTRL2033に伝える。

⑧アクセス要求⑦に対してアクセス権限チェックを行なう。権限がない場合、⑦の操作を無視する。

⑨アクセス要求⑦に対してアクセス権限チェックを行なう。権限がある場合、⑦の操作を汎用OS201に伝える。

【0017】

図4は、目的とするリソースに対するアクセス権限がある場合に、そのリソースを解放するまでのアプリケーション2021、リソース管理プログラム203

、汎用OS201のやり取りを示したAPIの監視及び制御の第1の基本型（1）のシーケンス図である。

この第1の基本型（1）では、アプリケーション2021から目的のリソースへのアクセス要求があった場合（ステップ401）、リソース管理プログラム203はアクセス権があるかチェックし（ステップ402）、アクセス権がある場合（ステップ403）、汎用OS201にアプリケーション2021が発行したAPIをそのまま伝える。汎用OS201は、OS本来のAPI処理を行なう（ステップ404）。

リソース管理プログラム203は、APIが成功した場合、アプリケーション2021がそのリソースを保持しているという情報を登録する（ステップ405）。そして、汎用OS201からのAPI結果をそのままアプリケーション2021に返す（ステップ406）。これにより、リソースへのアクセス完了となる（ステップ407）。

#### 【0018】

この後、アプリケーション2021から保持しているリソースの解放要求が発行された場合（ステップ408）、リソース管理プログラム203はその解放要求を汎用OS201に伝える。汎用OS201は、OS本来のAPI処理を行なう（ステップ409）。リソース管理プログラム203は、APIが成功した場合、アプリケーション2021がそのリソースを保持しているという情報を解除する（ステップ410）。そして、汎用OS201からのAPI結果をそのままアプリケーション2021返す（ステップ411）。これにより、保持しているリソースの解放完了となる（ステップ412）。

#### 【0019】

図5は、目的とするリソースに対するアクセス権限がなかった場合に、そのアクセスが拒否されるまでのアプリケーション2021、リソース管理プログラム203、汎用OS201のやり取りを示したAPIの監視及び制御の第2の基本型（2）のシーケンス図である。

この第2の基本型（2）では、アプリケーション2021から目的のリソースへのアクセス要求があった場合（ステップ501）、リソース管理プログラム2

03はアクセス権があるかチェックし（ステップ502）、アクセス権がなかった場合（ステップ503）、アクセス違反エラーをアプリケーション2021に返す（ステップ504）。これにより、リソースへのアクセス完了となる（ステップ505）。

また、アプリケーション2021がアクセス違反エラーに対応していないものにあつては、アプリケーション2021から目的のリソースへのアクセス要求があつた場合（ステップ506）、リソース管理プログラム203はアクセス権があるかチェックし（ステップ507）、アクセス権がなく、かつ、アプリケーション2021がアクセス違反エラーに対応していない場合（ステップ508）、リソース管理プログラム203が予め用意したダミーのリソースへのアクセス要求に置き換え、汎用OS201に渡す（ステップ509）。

#### 【0020】

汎用OS201は、OS本来のAPI処理を行なう（ステップ510）。リソース管理プログラム203は、汎用OS201からのAPI結果をそのままアプリケーション2021返す（ステップ511）。この結果、目的のリソースへのアクセス完了となるが、ダミーリソースのため、実質的には何も行われぬ（ステップ512）。

#### 【0021】

本発明は、以上のようにしてアクセス権限のないリソースへのアクセスを制限するものであるが、汎用のOSであるWindowsとUNIXの場合のAPIを例に挙げて説明する。

まず、ファイルへの複製を禁止する例について説明する。

ファイルへの複製については、従来、読み込み許可ファイルはファイルのコピーが可能であり、その結果オリジナルが複数存在したり、別媒体にて持ち出すことが可能であつた。本発明では、ファイルコピーを実現するAPIを監視／制御することにより、権限のないファイルのコピーを禁止する。その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。なお、以下で例示するAPIの機能については、各種の文献で公開されているので、その詳細な説明は省略する。

(1) ファイルオープン／作成API

CreateFileA  
CreateFileW  
OpenFile  
\_lopen  
\_lcreat  
GetOpenFileNameA  
GetOpenFileNameW  
GetSaveFileNameA  
GetSaveFileNameW

(2) ファイルクローズAPI

CloseHandle  
\_lclose

(3) ファイルコピー／移動API

CopyFileA  
CopyFileW  
MoveFileA  
MoveFileW  
MoveFileExA  
MoveFileExW  
DeleteFileA  
DeleteFileW  
DragQueryFileA  
DragQueryFileW

UNIXの場合、監視／制御するAPIとしては次のものがある。

(1) ファイルオープン／作成API

open  
creat

(2) ファイルクローズAPI

c l o s e

(3) ファイルコピー／移動 A P I

r e n a m e

【0022】

このような A P I の監視によってファイルへの複製を禁止する場合、具体的な方法として3つの方法がある。

＜方法1＞（ファイルオープン中に複製処理を行なうことが判明している場合）

アプリケーションが、複製権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションが別のファイルを作成することを拒否する。

＜方法2＞（ファイルクローズ後に複製処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、複製権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、複製権限のあるファイルをオープンするまで、そのアプリケーションが別のファイルを作成することを拒否する。

＜方法3＞（ファイルクローズ後に複製処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、複製権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションが別のファイルを作成することを拒否する。

なお、いずれの方法であっても、別に作成されるファイルによって複製が残ることがないと判明している場合（一時ファイルなどの作成）は拒否しない。

【0023】

次に、特定ファイルまたは全ての印刷を禁止する例について説明する。

従来、印刷機能を実装したアプリケーションによって、ファイルの内容を印刷し、外部に持ち出すことは可能であった。本発明では、印刷を実現する A P I を監視／制御することにより、権限のないファイルの印刷を禁止する。また F A X などその他の外部出力装置についても、それぞれのデバイスを監視／制御すること

により、同様に禁止する。その場合に、Windows及びUNIXにおいて監視／制御するAPIとして次のものがある。

Windowsの場合

(1) デバイスオープンAPI

CreateDCA

CreateDCW

(2) デバイスクローズAPI

ReleaseDC

ClosePrinter

(3) プリンタ選択／APL処理API

OpenPrinterA

OpenPrinterW

GetPrinterA

GetPrinterW

SetPrinterA

SetPrinterW

SendMessageA

SendMessageW

PostMessageA

PostMessageW

UNIXの場合

(1) デバイスオープンAPI

open

(2) デバイス制御API

ioctl

(3) デバイスクローズAPI

close

【0024】

このようなAPIの監視によって印刷を禁止する場合、具体的な方法として3

つの方法がある。

＜方法1＞（ファイルオープン中に印刷処理可能なことが判明している場合）

アプリケーションが、印刷権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープン拒否する。

＜方法2＞（ファイルクローズ後に印刷処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、印刷権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、印刷権限のあるファイルをオープンするまで、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープン拒否する。

＜方法3＞（ファイルクローズ後に印刷処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、印刷権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープン拒否する。

【0025】

次に、外部装置の利用を禁止する例について説明する。

従来、OSに装備されている機能や外部装置そのものに権限を付加することは、一般的にはできなかった。本発明では、監視／制御すべきAPIを限定できる機能の指定や、外部装置利用の指定をすることにより、その利用を禁止する。その場合に、Windows及びUNIXにおいて監視／制御するAPIとして次のものがある。

Windowsの場合

(1) デバイスオープンAPI

CreateFileA

CreateFileW

OpenFile

\_lopen

`_lcreat`

(2) デバイスクローズAPI

`CloseHandle`

`_lclose`

UNIXの場合

(1) デバイスオープンAPI

`open`

(2) デバイス制御API

`ioctl`

(3) デバイスクローズAPI

`close`

【0026】

例えば、このようなAPIの監視によって印刷を禁止する場合、具体的な方法として次の方法がある。

<方法>

アクセス権限テーブルにて、特定の条件のもとに特定デバイスの使用を禁止されている場合、そのデバイスの利用を以下の方法で拒否する。そのデバイスのデバイス名をもってデバイスオープンAPI要求があった場合、アクセス禁止エラー、もしくはデバイスが存在しないというエラーを返すことで要求を拒否する。

【0027】

次に、ファイル内の一部のデータまたは全ての複写を禁止する例について説明する。

従来、アプリケーションによってファイルを画面表示した結果、その内容のすべてまたは一部をOSの機能によって複写またはオブジェクトという単位で別ファイルに埋め込むことが可能であった。

本発明では、転写や埋め込み機能を実現するAPI（クリップボードのAPI、OLEのAPIなど）を監視／制御することで、権限のない流用を禁止する。その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。



## Windowsの場合

### (1) 複写／埋め込みAPI

```
OpenClipboard
SetClipboardData
GetClipboardData
GetOpenClipboardWindow
OleCreate
OleCreateEx
OleCreateFromFile
OleCreateFromFileEx
OleCreateFromData
OleCreateFromDataEx
OleCreateLink
OleCreateLinkEx
OleCreateLinkFromData
OleCreateLinkFromDataEx
OleCreateLinkToFile
OleCreateLinkToFileEx
CloseClipboard
```

### 【0028】

このようなAPIの監視によって複写を禁止する場合、具体的な方法として4つの方法がある。

<方法1> (ファイルオープン中に複写処理可能なことが判明している場合)

アプリケーションが、複写権限のないファイルをオープンし保持している間 (ファイルをクローズするまでの期間)、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

<方法2> (ファイルクローズ後に複写処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合)

アプリケーションが、複写権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、複写権限のあるファイルをオープンするまで、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

＜方法3＞（ファイルクローズ後に複写処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、複写権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

＜方法4＞（複写権限のないファイルを埋め込みオブジェクトとして取り込む場合）

複写権限のないファイルを取り込む処理を行なう際に、オブジェクトの登録もしくはそのオブジェクトの取得APIにおいて、アクセス違反のエラーを返すか、空データを登録あるいは取得することで、処理要求を拒否する。

#### 【0029】

次に、ネットワークを介してファイルが外部へ流出することを禁止する例について説明する。

従来、ファイルコピー以外に、FTPプログラムのように、ネットワークを介してファイルを外部へ転送することは可能であった。本発明では、ネットワークリソースにアクセスするAPIを監視／制御することで、権限のないファイルを使用中のアプリケーションから外部への流出を禁止する。その場合に、Windows及びUNIXにおいて監視／制御するAPIとして次のものがある。

Windowsの場合

WSAStartup

accept

bind

connect

gethostbyname

gethostbyaddr  
getprotobyname  
getprotobynumber  
getservbyname  
getservbyport  
getpeername  
getsockname  
gethostname  
getsockopt  
setsockopt  
recv  
recvfrom  
socket  
select  
send  
sendto  
WSASend  
WSASendTo  
WSAAsyncSelect  
WSAAsyncGetHostByAddr  
WSAAsyncGetHostByName  
WSAAsyncGetProtoByNumber  
WSAAsyncGetProtoByName  
WSAAsyncGetServByPort  
WSAAsyncGetServByName  
WSACancelAsyncRequest  
WSASetBlockingHook  
WSAUnhookBlockingHook  
WSACleanup

close socket

shutdown

UNIXの場合

accept

bind

connect

gethostbyname

gethostbyaddr

getprotobyname

getprotobynumber

getservbyname

getservbyport

getpeername

getsockname

gethostname

getsockopt

setsockopt

recv

recvfrom

socket

select

send

sendto

close socket

shutdown

【0030】

このようなAPIの監視によって外部への流出を禁止する場合、具体的な方法として3つの方法がある。

<方法1>（ファイルオープン中に出力処理可能なことが判明している場合）

アプリケーションが、外部出力権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションからの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

＜方法2＞（ファイルクローズ後に出力処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、出力権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、出力権限のあるファイルをオープンするまで、そのアプリケーションの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

＜方法3＞（ファイルクローズ後に出力処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、出力権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

ただし、その通信によってデータ出力されないことが判明している場合は、拒否しない。

#### 【0031】

次に、ファイルの内容のイメージを取得することを禁止する例について説明する。

OSの機能として画面全体や一部、またはウインドウ単位のハードコピーをイメージデータとして取得することが、一般的には可能であり、従来、そのイメージデータを流用、持ち出しすることができた。本発明では、画面内のイメージデータ取得APIを監視／制御することで、イメージデータ取得を禁止する。

その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

#### （1）デバイスオープンAPI

GetWindowDC

WindowFromDC

GetDC

GetDCEx

GetDesktopWindow

GetDeviceCaps

CreateDCA

CreateDCW

(2) イメージ取得API

BitBlt

StretchBlt

(3) デバイスクローズAPI

DeleteDC

ReleaseDC

【0032】

このようなAPIの監視によってイメージを取得することを禁止する場合、具体的な方法として3つの方法がある。

＜方法1＞（画面全体のハードコピーを拒否する場合）

現在画面上に表示されているウィンドウを所有しているアプリケーションが、ハードコピー取得権限のないファイルを保持している場合、画面全体のハードコピー取得を拒否する。画面全体のハードコピーは、画面全体を管理しているウィンドウ（Windowsの場合はデスクトップウィンドウ）を監視することで、＜方法2＞と同じ。

WindowsにおけるDirectDrawなど、画面全体のハードコピーを取得するAPIが存在すれば、同様に拒否する。

さらに、ディスプレイデバイスからVRAMイメージを取得するアプリケーションに対しては、それを拒否する。

＜方法2＞（ウィンドウのハードコピーを拒否する場合）

現在画面上に表示されているウィンドウを所有しているアプリケーションが、ハードコピー取得権限のないファイルを保持している場合、そのウィンドウのハードコピー取得を拒否する。ウィンドウが画面上に表示されているかは、ウィンドウの状態を監視することで行なう。

また、ハードコピー取得の拒否は、そのウインドウに関連付けられたデバイスコンテキストからのイメージコピーを拒否することで行なう。

＜方法3＞（画面の一部のハードコピーを拒否する場合）

ハードコピーを取得する領域が判断できる場合は、＜方法1＞における条件を、取得領域が対象となるウインドウと重なる時とし、以降は＜方法1＞と同じ。また領域が判断できない時は、＜方法1＞と同じ。

【0033】

次に、ファイル種別毎に利用アプリケーションを限定する例について説明する

従来、アプリケーション利用に制限がないため、参照以外の目的でファイルにアクセス可能であった。本発明では、ファイルごとに利用アプリケーションを限定できる。その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

(1) ファイルオープンAPI

CreateFileA

CreateFileW

OpenFile

\_lopen

\_lcreat

(2) ファイルクローズAPI

CloseHandle

\_lclose

(3) プロセス管理API

WinExec

CreateProcessA

CreateProcessW

ExitProcess

UNIXの場合

(1) ファイルオープンAPI

open

## (2) ファイルクローズAPI

close

## 【0034】

このようなAPIの監視によって利用アプリケーションを限定する場合、具体的な方法として次の方法がある。

## &lt;方法&gt;

アプリケーションがファイルをオープンする際、そのファイルの権限をチェックし、許可されたアプリケーションでない場合はアクセス違反エラーを返すことで、オープン要求を拒否する。

次に、OSの特定の機能の利用を禁止する例について説明する。

従来、OSに装備されている機能に権限を付加することは、一般的にはできなかった。本発明では、監視／制御すべきAPIを限定する機能を指定することで、その利用を禁止することができる。例えば、ファイルのタイムスタンプやシステム日時の変更を禁止するなどである。その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

## (1) ファイルのタイムスタンプ変更API

SetFileTime

## (2) システム日時の変更API

SetSystemTime

SetSystemTimeAdjustment

## 【0035】

このようなAPIの監視によってOSにおける特定の機能の利用を禁止する場合、具体的な方法として次の方法がある。

## &lt;方法&gt;

特定の条件下で禁止されているAPIが発行された際に、アクセス違反エラーを返すか、実際の処理を行わずに（ダミー処理）正常リターンすることで、禁止されているAPI（OS機能）を拒否する。

## 【0036】



次に、プロセス内メモリの参照または変更を禁止する例について説明する。

従来、アプリケーションが明示的に拒否しない限り、プロセス内メモリの参照／変更を禁止することができなかった。本発明では、プロセス内メモリの参照／変更APIを監視／制御することで、他のアプリケーションからの参照／変更を禁止することができる。

その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

(1) プロセス管理API

OpenProcess

CreateProcess

CloseHandle

(2) メモリ操作API

ReadProcessMemory

WriteProcessMemory

ReadProcessMemoryVlm

WriteProcessMemoryVlm

【0037】

このようなAPIの監視によってプロセス内メモリの参照または変更を禁止する印刷を禁止する場合、具体的な方法として次の方法がある。

<方法>

アクセスが禁止されているアプリケーションのプロセス内メモリにおいて、メモリ操作APIが要求された際に、アクセス違反エラーを返す。

次に、ブラウザに表示したWebページの印刷や保存や外部装置への出力を禁止する例について説明する。

従来、閲覧や再生のみを許可したWebページでも、実際にはブラウザソフトウェアによって印刷や保存が可能であった。WebページをロードするためのネットワークリソースにアクセスするAPIを監視し、ブラウザが行う印刷や保存のアプリケーションを監視／制御することにより、印刷や保存や外部装置への出力操作を禁止することができる。その場合に、監視／制御するAPIとして次のような

ものがある。

Windowsの場合

(1) 通信API

WSAStartup

accept

bind

connect

gethostbyname

gethostbyaddr

getprotobyname

getprotobynumber

getservbyname

getservbyport

getpeername

getsockname

gethostname

getsockopt

setsockopt

recv

recvfrom

socket

select

send

sendto

WSASend

WSASendTo

WSAAsyncSelect

WSAAsyncGetHostByAddr

WSAAsyncGetHostByName

WSAAsyncGetProtoByNumber  
WSAAsyncGetProtoByName  
WSAAsyncGetServByPort  
WSAAsyncGetServByName  
WSACancelAsyncRequest  
WSASetBlockingHook  
WSAUnhookBlockingHook  
WSACleanup  
closesocket  
shutdown

(2) その他、前述のファイル、印刷、外部装置への操作を禁止する場合のA

PI

UNIXの場合

(1)

accept  
bind  
connect  
gethostbyname  
gethostbyaddr  
getprotobyname  
getprotobynumber  
getservbyname  
getservbyport  
getpeername  
getsockname  
gethostname  
getsockopt  
setsockopt  
recv

recvfrom  
socket  
select  
send  
sendto  
closesocket  
shutdown

(2) その他、前述のファイル、印刷、外部装置への操作を禁止する場合の API

【0038】

このような通信 API を監視し、印刷や保存や外部装置への出力を禁止する方法として、次の方法がある。

まず、Web ページ内に記述された禁止指定を読み取る。具体的には、http プロトコルまたは同等のプロトコルのデータを監視し、その中の Web ページデータ部分に印刷や保存の禁止指定タグが含まれていれば、その Web ページは印刷や保存が禁止されていると判断する。または、権限の獲得を利用者に求め、獲得できなかった場合に印刷や保存が禁止されていると判断する。しかし、獲得できた場合には、印刷や保存が禁止されていないものと判断する。すなわち、アクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する。

印刷や保存や外部装置への出力が禁止されているページを表示しているブラウザが、印刷や保存を行なおうとした場合、前述した印刷やファイルの保存や外部装置への出力を禁止する方法を用いて、それを禁止する。

ここで説明した Web ページの例は、そのしくみの類似性により、容易にデジタルテレビジョンのコンテンツにおいても利用できるものである。

【0039】

次に、リソース管理プログラムを応用した例を示しておく。

図6は、リソース管理プログラム203が管理しているリソースのアクセス状況を履歴管理プログラム601に転送し、履歴管理データベース(DB)602

に格納しておき、必要に応じて、図 8 に示すようなアクセス監視履歴として画面表示する構成を示したものである。通報プログラム 6 0 3 は、不正なアクセスがあった場合にシステム管理者の端末に対し、図 7 (b) で示すような内容の不正アクセス通知画面を送信し、表示させるものである。

なお、一般ユーザが不正アクセスを行なった場合には、図 7 (a) で示すような画面表示が行われる。

#### 【 0 0 4 0 】

なお、上記の説明においては、アクセス権管理テーブルを参照してアクセス権限の有無を判定するようにしているが、コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定するようにすることもできる。

また、上記の説明において用いたネットワークリソースとは、通信媒体、デバイス、アクセスポイント、ディジタルテレビジョンのチャンネル、通信データまたはコンテンツなど、OS が管理しているリソースのうちネットワークに関するものである。

#### 【 0 0 4 1 】

以上のように、本実施形態においては、基本的には、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定し、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否するようにしたため、OS やプロセス (OS の元に稼動しているプログラムであり、アプリケーションやデーモンなど) を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限することができる。

また、リソース管理プログラムを既存の環境に組み込むだけで、上述したような各種の不正アクセスを制限することができ、既存のアクセス権の範囲を拡張す

ることが可能になる。

【0042】

さらに、要求元のアプリケーションがアクセス違反に対応する機能を有していない場合であっても、ダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡すようにしたため、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができる。

【0043】

なお、リソース管理プログラムは、CD-ROM等のディスク型ストレージ、半導体メモリ及び通信ネットワークなどの各種の媒体を通じてコンピュータにインストールまたはロードすることができる。また、プログラム製品単体として、コンピュータユーザに提供することができる。

また、実施形態で例示したAPIについては、その一例を示しただけであって、OSのバージョンアップなどによって追加された場合でも容易に対応できることは言うまでもない。

【0044】

【第2実施形態】

図10は本発明による第2の実施形態をしめす。図10の11は、先に説明したセキュリティ環境における本発明のコンピュータアーキテクチャの構造を示す。本構成は、ハミングヘッズセキュリティ管理方式（HHシステム）の全体構成を示すもので、本発明による、コンピュータアーキテクチャのHierarchyを示した。

【0045】

17はOSで先に説明したようにWindowsでも、MACでもOSはどれでもよい。OSに依存しないのが特徴である。18のAPI1（Application Program Interface 1）は、OSの中に位置していて、OSとのインターフェースの役割を果たす。19のSCMからの要求に応じて、OSに指示をおくる。

この場合の指示とは、クライアントへの情報の提供の方法に関するものであって、情報を一切拒否したり、閲覧のみ可としたり、コピー、メール、転送等の許

可を行う。

【0046】

19のSCM (Security Control Management) は、本発明の主旨であってH. H (ハミングヘッズ) セキュリティモジュールを示す。

OS、APL (アプリケーション・ソフトウェア) の処理を監視している。

何らかの条件で、許可、不許可を決める。12の管理テーブルがあって、本システムにどのような形でクライアントがアクセス可能か、クライアントがアクセスした場合、管理テーブルの中に人の名、電話番号、あるいはID番号でアクセスしたクライアントの位置付けと重みを判断する。

【0047】

クライアントの要求をそのまま受け入れるか、条件をつけて許可するかは、12に格納されているクライアントの個人データによって判断する。

情報の提供を要求どうりクライアントに提供できないが、課金する事によって提供できる事もある。図11にSCM19の位置付けの模式図を示している。

【0048】

図10の20のAPI2 (Application Program Interface 2) は、クライアントのアクセスを監視していて、アクセスがあればOSにわたす。

OSのコントロール下にある外部デバイスの監視もおこなう。OSの要求する全てのリソースが対象になる。

【0049】

14のファイルは、20のAPI2に接続されていて、クライアントからのアクセス、要求の履歴を記憶する。

【0050】

21のAPLは各種のアプリケーションプログラムであって、例えばマイクロソフト社のOffice2000、Word、Excel、Power Pointなどの類である。クライアント、ユーザは文章、図、あるいは静止画、動画、音声、音楽等のOSのコントロール下で行う。13は21のファイルで各種の

アプリケーションソフト、クライアント、ユーザの作成した創作物を格納する。

【0051】

図10の22は本サーバ、サイトと外部デバイスとを接続するインターフェースで、本例では、通信ネットワーク15、ドライバーソフト16を介してクライアント、ユーザの画面23、プリンター24、Fax／コピー機25に接続している。

又、クライアント、ユーザは通信ネットワーク15を介して、PC等を接続して23、24、25等のデバイスを用いて情報の提供を受けることが出来る。

【0052】

図10の26は、公衆網通信インターフェース、27は外部装置接続用のUSB、RS232C、IEEE1394等のシリアル、パラレルのコネクターと接続するラインである。29は外部接続機器との接続線であって、16のドライバーソフトは、外部機器23、24、25、28か11に内蔵されているのが一般的である。

【0053】

図11は、OS、外部装置、情報を格納してあるファイルと本発明によるSCMとの関係を示した模式図である。ユーザ、クライアントによって作られた創作物、H. Hサイト（ハミングヘッズサイト）、サーバから提供される各種の情報は13に格納してある。

この情報とは、文章、図、絵、音声、静止画、動画等を含む。

【0054】

SCM19はOS17とAPL21の中間に位置して情報の抽出、使用について、クライアント、ユーザの動きを監視している。OSのコントロール下で外部装置23、24、25、28への情報の出力についてクライアント、ユーザの権限をチェックして、制限をくわえる。制限とは、先に説明したように情報のコピー、メール、転送の許諾権を与えるものである。

【0055】

SCM19に接続しているファイル12には、クライアント、ユーザの権限情報を格納していて、要求に応じてその都度、照合して外部装置、デバイスへの出



力に制限をくわえる。クライアント、ユーザはあらかじめ個人の情報を登録しておく必要がある。企業、法人、政府機関、自治体等であれば、部長、課長、一般職というように職位によって権限を制限したり、与えたりしてもよい。

【0056】

又、外部の一般人がクライアント、ユーザとしてアクセス要求がある場合もある。その時には、外部に出せる情報であれば無料のものと有料のものとを層別してSCM19が管理しておけばよい。

【0057】

### 【第3実施形態】

図12は第3の実施形態を示すシステム構成図である。通信ネットワーク15は、公衆網でINNTアーネットIP、電話網PSTN、XDSL網、デジタル網ISDN、B-ISDN、ATM、モバイル網、衛星網等を使用している。

31は公式のWebサイトで例えばNTTドコモ社のiモードのサイトがある。32はモバイル無線網のアンテナで、本実施例ではiモードサイトに接続している。もちろんPHS、他のPDC(Personal Digital Cellular)も使用できる。特にIMT2000は高速なので動画の伝送に優れている。

【0058】

33は本発明によるH. Hサイトで情報提供を行う。先に説明したようにセキュリティを万全にしたシステムであって、ユーザ、クライアントの権限によって制限を設けるものである。H. HサイトはSCM19をインプリメントしたソフトを搭載したサーバを使用している。

【0059】

34はデータベースのサイトであって各種のビジネス、研究等に必要な情報が格納してあって、H. Hサイトを介して使用できる。35はWebキャストでデジタル放送をH. Hサイトを通して利用できる。36は金融機関のサイトでH. Hサイトを使用して課金された場合、使用料の徴収をおこなう。

【0060】

37はWeb上に設けられたモールで、H. Hサイトを通してショッピングが

できる。購入の支払いは36の金融機関のサイトよりおこなう。

Web上で商品を買ったり、デジタル放送を見たり聞いたりして、課金が発生したときにはH. Hサイトを介しているので、利用者であるクライアント、ユーザそれにサービスの提供者はセキュリティが万全であるから安心して使用できる。

#### 【0061】

図12の38は利用者のための端末機器をコンビニ、街角、広場に設置した例である。図示してないがプリンター、コピー機等も接続している。

39は学校、研究機関を、40は工場、オフィスを示す。

41は一般家庭での使用例で45は、ホームサーバを示す。近年、在宅で仕事をする人がふえてきた。通信回線の発展の恩恵によるものであって、企業内のデータ、情報を活用する場合本発明によるセキュリティの効果が発揮する。46はホームルータである。

#### 【0062】

図12の42は携帯情報端末機器でモバイル機器ともいう。携帯電話機の普及は顕著で、特にiモードの発展は急速にたちあがった。CHTMLのブラウザにメールが可能で、これをもってH. Hサイトにもアクセスできるから利便性はよい。さらにPalmOSに見られるようにPDA（携帯情報機器）の使い勝手もよい。プリンター、インターネットカメラ、デジタルカメラを搭載したり接続もできる。

#### 【0063】

43はクライアント、ユーザである。図12ではモバイラーとして43の人は場所を問わず、何処ででも仕事ができる。当然H. Hのセキュリティである権制限機能が発揮されるから、図示してない企業のイントラネットも容易に使用できる。

#### 【0064】

44は車載移動体で、モバイルインターネットによって同様にH. Hサイトからのサービスを受けることができる。先に説明したようにH. Hサイトをはじめ、H. Hサーバも図11の19のSCMの機能によって安全に情報の管理が出来

る。

【0065】

【第4実施形態】

図13は第4の実施形態をしめす。企業内のイントラネットに本発明を応用した例である。配信ネットワーク15より26の回線を介してルータ51に接続されている。52はWWWサーバで53はファイアウォールである。53を介して本セキュリティを搭載したサーバ55に接続される。55はH. Hサーバである。

【0066】

56は55とLAN54で接続されている企業のデータベースである。このデータベースには、顧客のリスト、営業情報、工場であれば生産、製造の技術情報、設計開発の情報等企業活動に必要な各種のデータ、情報が格納されていてクライアントである企業の社員は先に説明したような、権限に応じて制限して利用できる。職能階層に応じて利用できる情報とできない情報がある。場合によっては代表権のある役員しか開示できない情報もあって、55のサーバに搭載されたH. H方式によって管理されている。

【0067】

企業内LAN54を介して接続してある57、58、59mnは、企業内のクライアントPC、サーバである。59は多機能電話機、60はプリンター、FAX/コピー機である。61は携帯情報端末機器、PDAを62は携帯電話機63はモバイルノートPCを示す。これらの機器は社内、構内モバイル機器として用いる。65は構内移動車載端末を示す。

64は企業内、構内モバイル端末機器用のアンテナを示す。

【0068】

本イントラネットは、企業だけでなく法人、研究機関、教育機関でも使用できるのをはじめ、企業外からもアクセスできる。外からの使用はセキュリティを確保して内部の情報を出すことが可能になる。本発明によるシステムはきわめて有効である。

【0069】

## 【第5実施形態】

図14は第5の実施形態をしめす。ホームでの実施例を示す。先に説明したようにITの普及によって、家庭で就労する人が増えてきた。我が国でもすでに6百万人を越えたと言われている。少子高齢化と伴にこの傾向は増加の一途にあるといえる。

## 【0070】

図14において、26の公衆回線よりホームルータ72に接続される。15はここでは公式Webサイトに接続している。例として、NTTドコモ社のiモードサイトがある。72のルータはホームLAN73に接続されている。73は有線LANだけではなく、ブルートース、Irdaを使用した無線LANでもよい。74はPCまたはホームサーバ、75は大画面付きの多機能電話機、76はTV、77は音響AV機器、78はモバイル携帯情報端末機器を示す。71はアンテナで公衆無線網との接続を行う。41は家、家庭を示す。

## 【0071】

在宅就労は各種の企業情報、機密情報を扱うのでセキュリティの確保は最重要課題である。公式Webサイト31を介して33のH. Hサイトを通して情報の授受を行うから安全である。又、仕事だけでなく娯楽としてのコンテンツをネットワークから配信を受ける環境になってきた。35のWebキャストからTVや音楽の配信を受けて、76のTV端末、77のAV機器、78の家庭内モバイル端末で楽しんで、生活を豊かにすることができる。

## 【0072】

娯楽コンテンツをネットワーク上のサイトから提供を受けた場合、料金の支払いが生ずる。33のサイトで管理されているからクレジットカード番号を入力して36の金融機関のサイトから自動引き落としが可能になる。この場合、なりすましを防止するために個人認証が必要になる。個人認証の方法は各種提案されているが、ID番号、電話番号のほかに機密度の高い場合は公開鍵を使用するのもよい。なお、74のホームサーバに本発明のSCMを搭載して安全を確保してもよい。組織に属して家庭で就労する場合、74のサーバは企業から提供されたものを使用して家庭就労するという、条件を設けるのも一つのホームワーキングの

方法である。

【 0 0 7 3 】

図 1 5 は本発明によるセキュリティ確保についての流れ、ユーザ、クライアントに制限と課金を課すことを説明するフロー図である。

S 8 1 はユーザ、クライアントが情報を得るためにサイトにアクセスする。S 8 2 は H. H サイト、H. H サーバにある SCM によってアクセスしてきたクライアント、ユーザの個人情報を検索、照合する。

【 0 0 7 4 】

S 8 3 はクライアント、ユーザからの情報の特定を行う。ここでいう特定とは、機密性の程度と、アクセスしてきたクライアントの職位の階層によって権限の制限を受けるのが特徴である。クライアント、ユーザは組織に所属しているものであれば、職位の階層は自動判別できる。一般からのアクセスも可能であるから提供できる情報と出来ないものを区別する。また無料で提供できる企業のカatalog 類とか宣伝類のほかに有料で頒布できる情報もある。有料でも価値の高いものは、課金の程度を変えて頒布するのを特徴とすれば、本 H. H サイトはビジネスとして成立する。

【 0 0 7 5 】

S 8 4 では H. H サーバまたはサイトにアクセスして来た、クライアント、ユーザからの要求にこたえられるか、SCM にある個人情報と照合して判定する。

【 0 0 7 6 】

S 8 5 では判定の結果、そのクライアントは情報を提供しても良い人であった。従って OK の返事、表示を出す。次に S 8 6 では、要求情報のコピーとメールで他人への転送の可否を聞いて来た。S 8 7 ではクライアントの職責、権限を SCM によってチェックする。先に説明したが、本発明では個人の権限によって情報の利用を制限するものである。

【 0 0 7 7 】

S 8 8 ではコピーもメール転送も OK と判定された。このクライアントは、高位的な権限をもっているか、要求情報の機密性の低いものであったと判断される。

S 8 9 では、クライアント、ユーザの誰それがどんな情報、ドキュメントをい

つ、コピーしたか、メール転送したかの履歴がH。Hサーバ、サイトに記録される。

【0078】

S90はH。Hサーバ、サイトでの履歴の管理も終わり、情報、ドキュメントの提供する体制が整った。クライアントへ情報を提供する。

【0079】

S91ではアクセスして来たクライアントの要求がS84の判定によって拒された。S92ではクライアントはID番号を、もし初めてアクセスして来た人とか一般の人であれば身分を証明する、電話番号、保険証の番号、免許証、年金番号等を入力する。

【0080】

お金を払えば提供できる情報もある。課金の金額をクライアントに知らせる。金額は情報、ドキュメントの機密度、重要度によって価値は変わる。従って金額も異なる。

S93では課金されてもH。Hサーバ、サイトの方で提供できない情報もある。又、クライアントの方でも課金されたら不要であったり、課金の金額によっては入手したいという人もいる。いずれにしても、入手の許可があればS85へ進む。なければこの処理を終了する。

【0081】

S94では、欲しい情報、ドキュメントのコピー、メール転送がS87の判定によって不可と判定された。クライアント、ユーザへ画面で見るとは、許可されている。見るだけの情報がクライアントに送られるが、SCM19によってOSをコントロールしているからクライアントの端末に表示されていても、コピーとメールの転送はできない。

【0082】

S95ではH。Hサーバ、サイトに先に説明したような履歴を管理する。S96ではクライアントの画面に要求のあった情報が表示される。どうしてもコピー、メール転送したい情報もある。ここであらためてサイト、サーバに許可の要求をだす。S97では、課金して情報の入手を申請する。このステップではクラ

クライアントの職責、階層は、H. Hサーバ、サイトに認知されているから金額の程度によって、許可できる場合もある。

【0083】

課金すれば提供できるとサイト、サーバが判断した場合、金額を提示する。課金しても提供できないとサイト、サーバが判断すればこの処理はクライアントへの画面表示S98のみで終了する。情報、ドキュメントの程度に応じて表示時間に制限を加えてもよい。所定時間内の表示を行って、より長時間見たい場合は課金制度を導入するのも一方法である。

【0084】

この場合、S99、S100でH. Hサイト、サーバからより長時間の表示と課金の有無をクライアント、ユーザに問い合わせる。H. Hサーバ、サイトとクライアントが了解すればS101で画面表示を長時間行う。

【0085】

H. Hサーバ、サイトの課金とクライアント、ユーザの了解が得られない場合は所定時間のみの表示S98でこの処理は終了する。

【0086】

以上説明したように、第1実施形態ではアクセス権限をOSやそのプロセスを変更しないでユーザ、クライアントに対して制限して不正行為を防止する例を、第2実施形態では、H. Hサイト、サーバのシステム構成を、第3実施形態では通信ネットワーク、特にインターネットを中心にして社会環境で発揮するH. Hサイトのシステム構成をしめす。

【0087】

第4実施形態では企業内、工場、学校、研究機関、団体等のイントラネットに本H. Hサーバの応用について示し、第5実施形態では、ホームオフィス、在宅就労における本H. Hサイトの応用について示した。

【0088】

なお、図15のフロー図はH. Hサーバ、サイトを介して情報、ドキュメントの閲覧、コピーメール転送について説明してあるが、図12のWebキャストからのデジタル放送の配信、各種無料有料コンテンツからの配信による課金システ

ムにも適用する。

【 0 0 8 9 】

【発明の効果】

以上の説明から明らかなように、本発明は、基本的には、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定し、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否するようにしたため、OSやプロセス（OSの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限することができる。

また、リソース管理プログラムを既存の環境に組み込むだけで、上述したような各種の不正アクセスを制限することができ、既存のアクセス権の範囲を拡張することが可能になる。

また、リソース制御プログラムを既存の環境に組み込むだけで、各種の不正アクセスを制限することができ、従来のアクセス権の範囲を拡張することが可能になる。

さらに、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができるなどの効果が得られる。

【 0 0 9 0 】

急速に進展しているeビジネスに本発明による権限制限システムを応用すれば、不正アクセスの防止、各種有料コンテンツの配信による課金に効力を発揮する。急激な高齢化社会の到来に伴い在宅就労も重要な課題になってきた。

本H. Hシステムの導入によって、安全に企業のドキュメント、データ、情報が家庭内で取り出せて、家庭内作業と成果をWebサイト、企業に送る事も可能になった。



【図面の簡単な説明】

【図 1】

本発明の実施環境の第 1 実施形態を示すハードウェア構成図である。

【図 2】

本発明に係るリソース管理プログラムの機能構成及び OS とアプリケーションとの関係を示す図である。

【図 3】

アクセス管理テーブルのデータ構成例を示す図である。

【図 4】

本発明における API の監視／制御の第 1 の基本型を示すシーケンス図である。

【図 5】

本発明における API の監視／制御の第 2 の基本型を示すシーケンス図である。

【図 6】

アクセス履歴を記録する機能を示すブロック構成図である。

【図 7】

不正アクセスを示す画面例である。

【図 8】

アクセス監視履歴の表示画面の例を示す図である。

図である。

【図 9】

アクセス制限対象となるリソースの例を示す図である。

【図 10】

H、H サイト、サーバの構成を示す第 2 実施形態の図である。

【図 11】

SCM と OS、ファイル、外部装置との関係を示す図である。

【図 12】

全体のシステム構成を示す第 3 の実施形態の図である。

【図 13】

イントラネットへの応用を示す第4の実施形態である。

【図 14】

ホームでの応用を示す第5の実施形態である。

【図 15】

ユーザ、クライアントへの制限と課金のプロセスを示すフロー図である。

アクセス制限対象となるリソースの例を示す図である。

【符号の説明】

- 101 コンピュータ
- 102 ネットワーク
- 201 汎用OS
- 203 リソース管理プログラム
- 601 履歴管理プログラム
- 603 通報プログラム
- 2031 API監視コントローラ
- 2032 APL監視コントローラ
- 2033 アクセス制御コントローラ
- 2034 OS監視コントローラ
- 2035 アクセス権管理テーブル
- 11 H. Hサーバのアーキテクチャ
- 12 管理テーブルファイル
- 13 アプリケーションソフトウェアのファイル
- 14 アクセス履歴記録、管理ファイル
- 15 通信ネットワーク
- 16 外部装置ドライバソフト
- 17 汎用OS
- 18 API1 (Application Program Interface 1)
- 19. SCM (Security Control Management)

20 API2 (Application Program Interface 2)

21 APL (Application Program Logic)

22 外部機器インターフェース

23 画面端末装置、TV、PDA、大画面付多機能電話機

24 プリンター

25 Fax／コピー機

26 通信ライン

27 コネクター、ケーブル

28 PC、サーバ

31 公式Webサイト

32 無線基地局

33 H. H (ハミングヘッズ) Webサイト

34 データベースサイト

35 Webキャスト、デジタル放送局

36 銀行、金融機関、クレジット会社

37 Webモール、インターネットショップ

38 コンビニ、街角ターミナル

39 学校、研究機関

40 企業、工場、オフィス

41 家庭、在宅就業

42、78 携帯情報端末機器、携帯電話機、PDA

43 ユーザ、クライアント

44 車載移動端末機器

45、74 ホームサーバ

46、72 ホームルータ

51 ルータ

52 Webサーバ

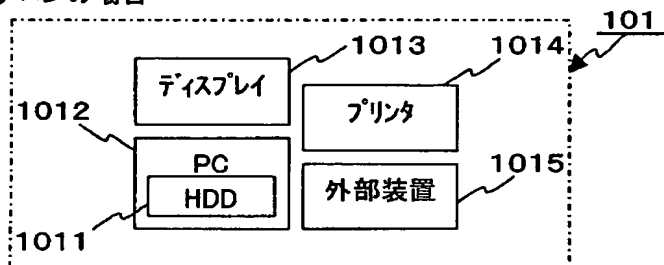
53 ファイアウォール

- 54 LAN (Local Area Network)
- 55 H. Hサーバ
- 56 情報格納ファイル
- 57, 58, 58mn PC、サーバ
- 59、75 多機能電話機
- 60 Fax、プリンター、コピー機
- 61 携帯情報端末機器
- 62 携帯電話機
- 63 ノートPC
- 64 構内無線アンテナ
- 65 構内移動車載端末機器
- 66、67 接続線
- 71 ホーム無線アンテナ
- 77 音響機器
- 76 TV

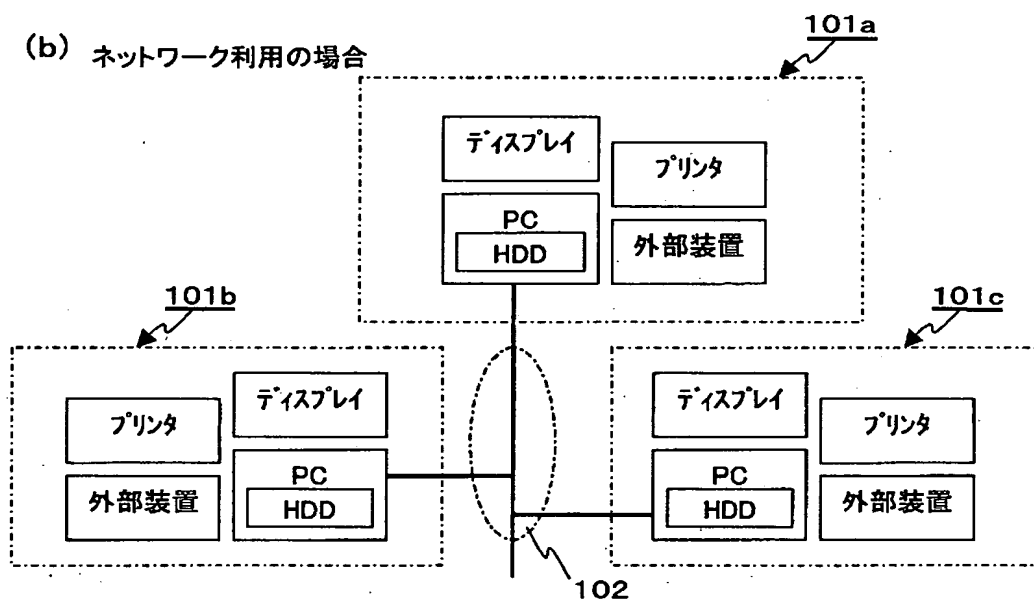
【書類名】 図面

【図 1】

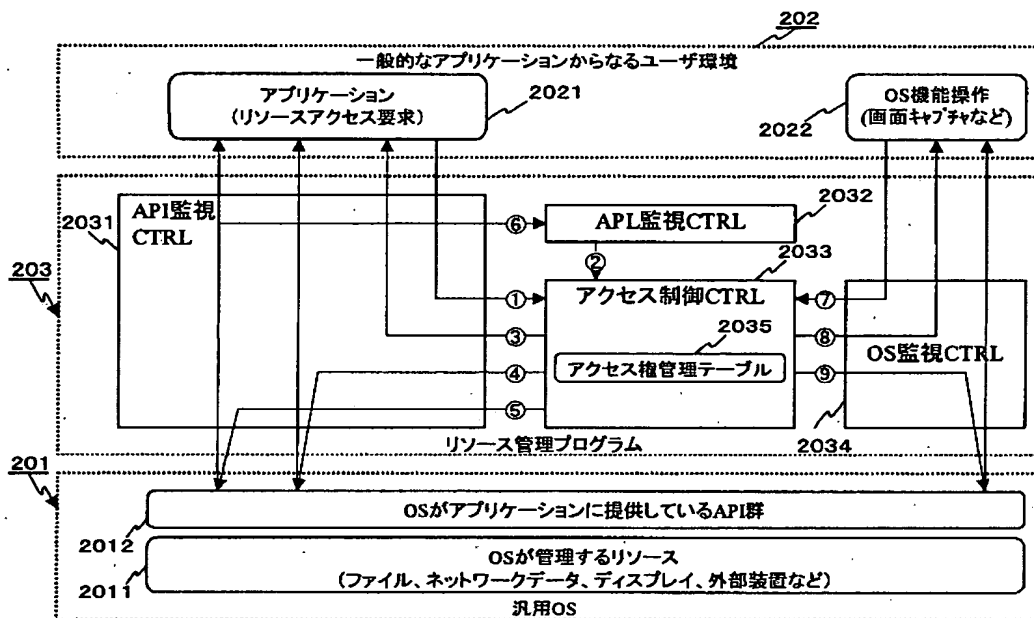
(a) スタンドアロンの場合



(b) ネットワーク利用の場合



【図 2】



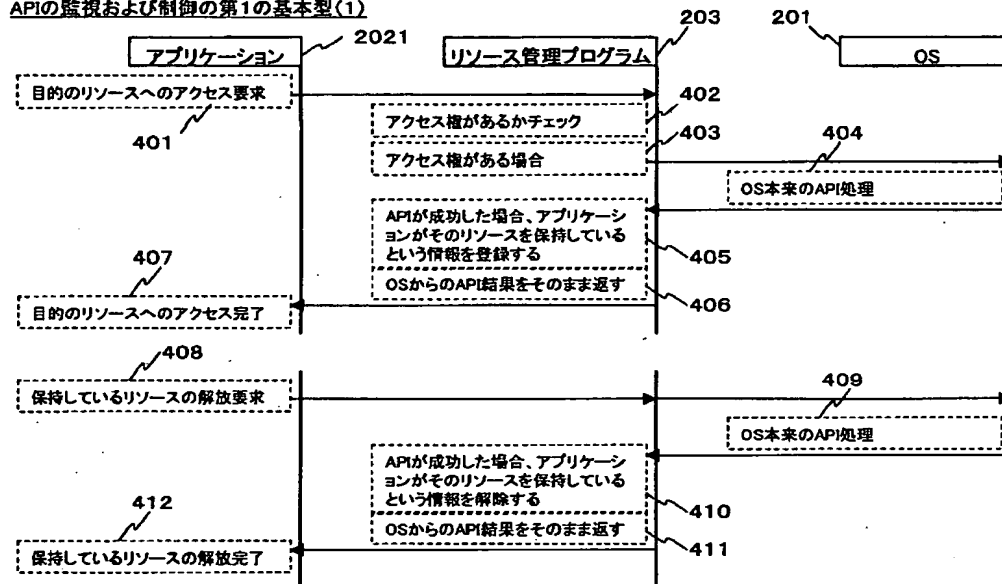
【図 3】

アクセス権管理テーブル

20351	20352	20353	...	2035n
リソース指定情報A	条件A	アクセス権情報A1	...	アクセス権情報An
リソース指定情報B	条件B	アクセス権情報B1	...	アクセス権情報Bn
リソース指定情報C	条件C	アクセス権情報C1	...	アクセス権情報Cn

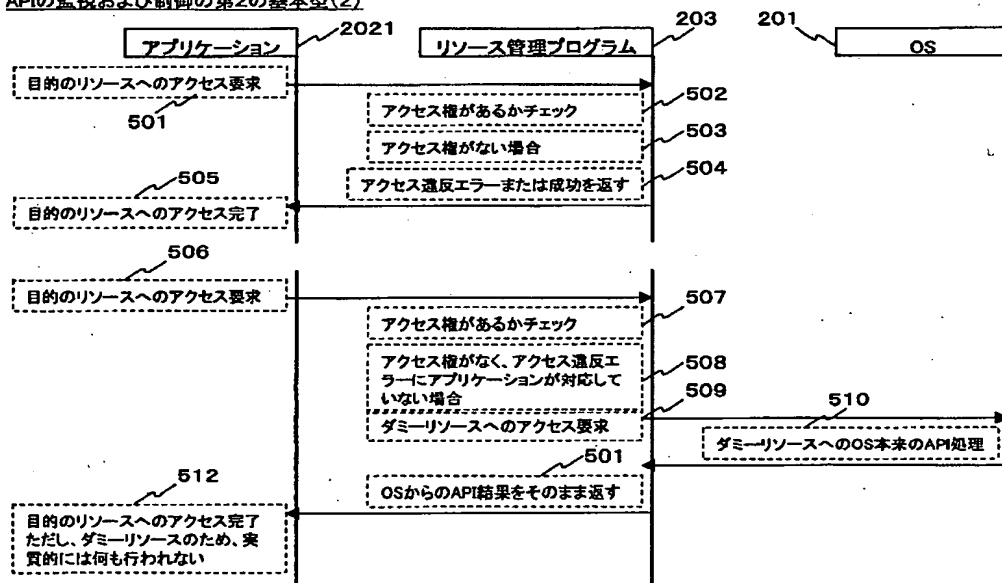
【図 4】

APIの監視および制御の第1の基本型(1)

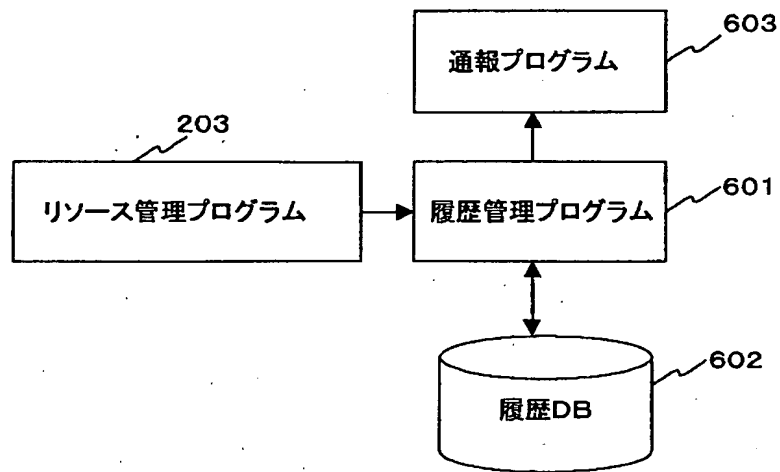


【図 5】

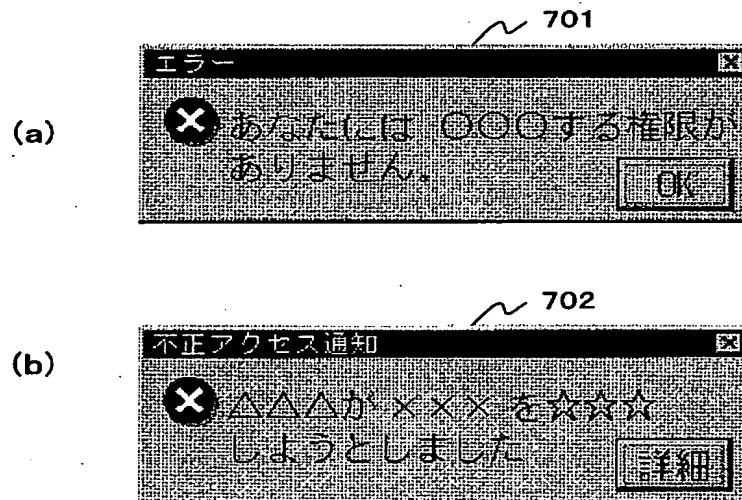
APIの監視および制御の第2の基本型(2)



【図 6】



【図 7】





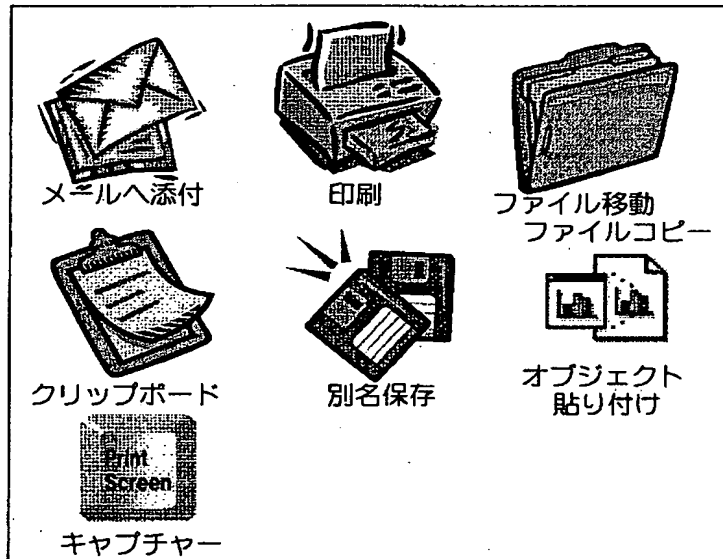
【図8】

801

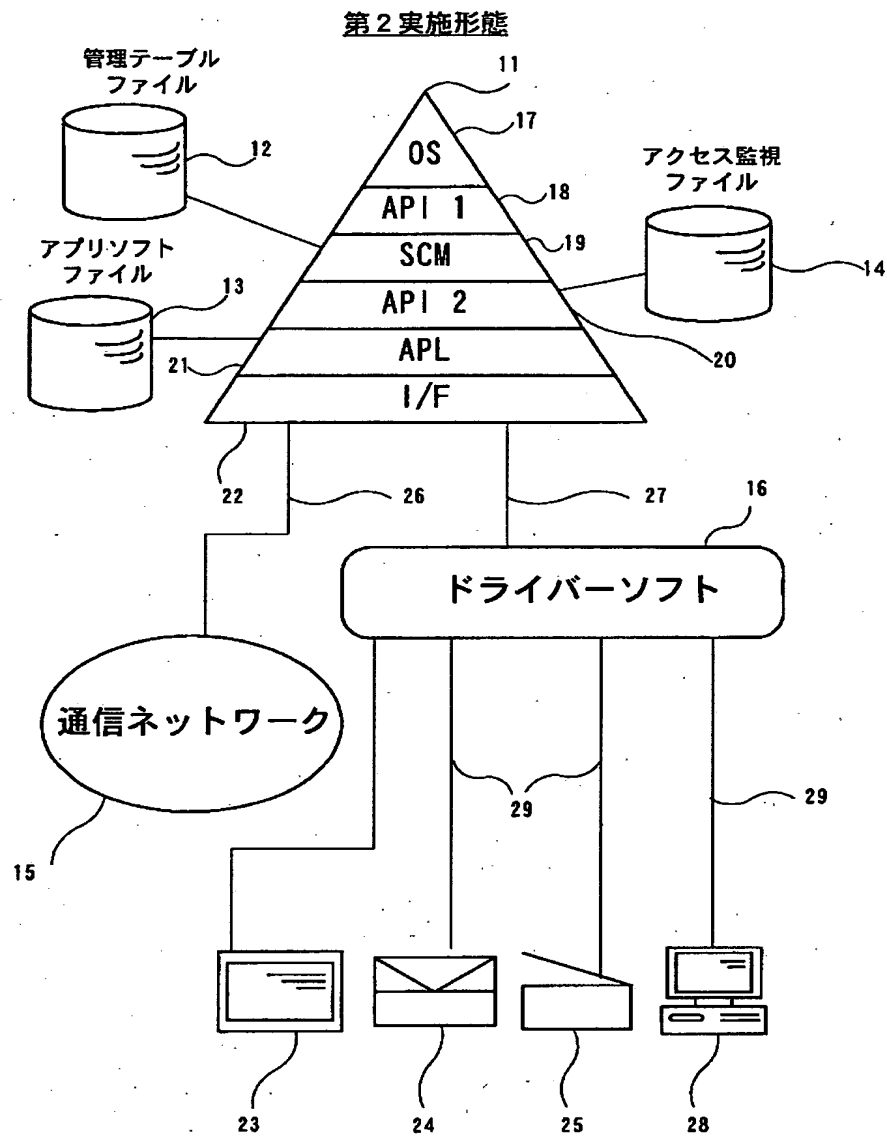
ファイル名	利用者	操作	アクション	アクセス日時	場所
機密文書	〇〇〇さん	ファイル更新	許可	00/01/01 0:00	総務...
顧客リスト	◆◆◆さん	印刷	拒否	00/01/01 0:00	営業...
開発ソース	☆☆☆さん	ファイルコピー	失敗	00/01/01 0:00	開発...
進行表	???さん	文書内部コピー	成功	00/01/01 0:00	企画...
査定表	●●●さん	メール添付	拒否	00/01/01 0:00	人事...
財務報告書	□□□さん	画面キャプチャー	許可	00/01/01 0:00	経理...
会社案内	×××さん	ファイル移動	失敗	00/01/01 0:00	営業...
組織図				00	総務...

権限の無い◆◆◆さんが顧客リストを印刷しようとしたので拒否しました。

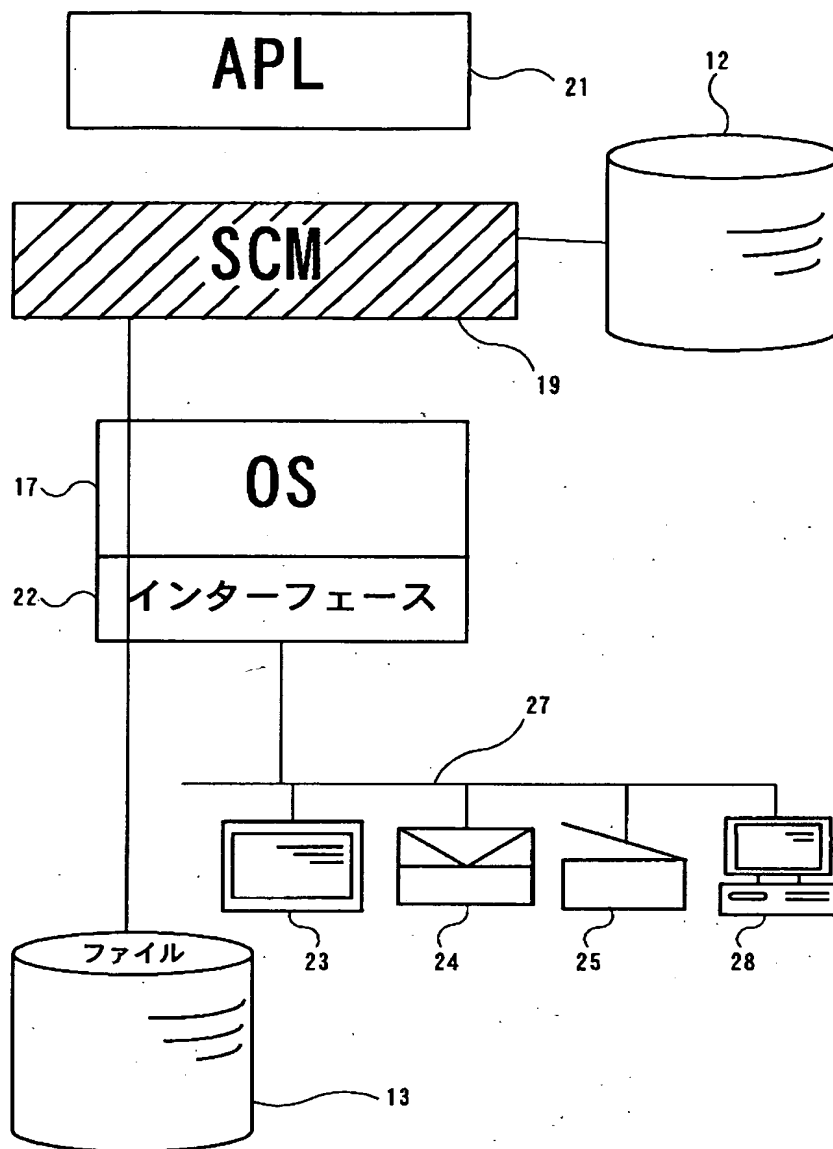
【図9】



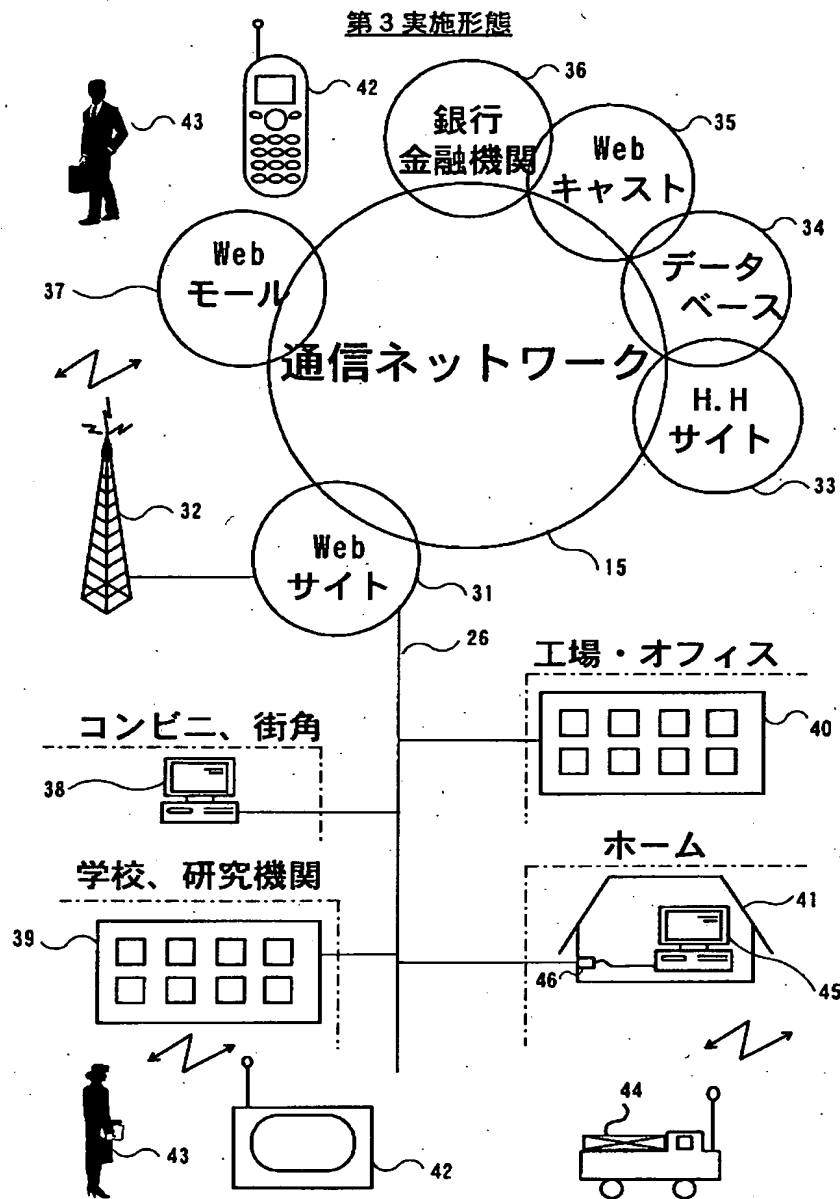
【図10】



【図 11】

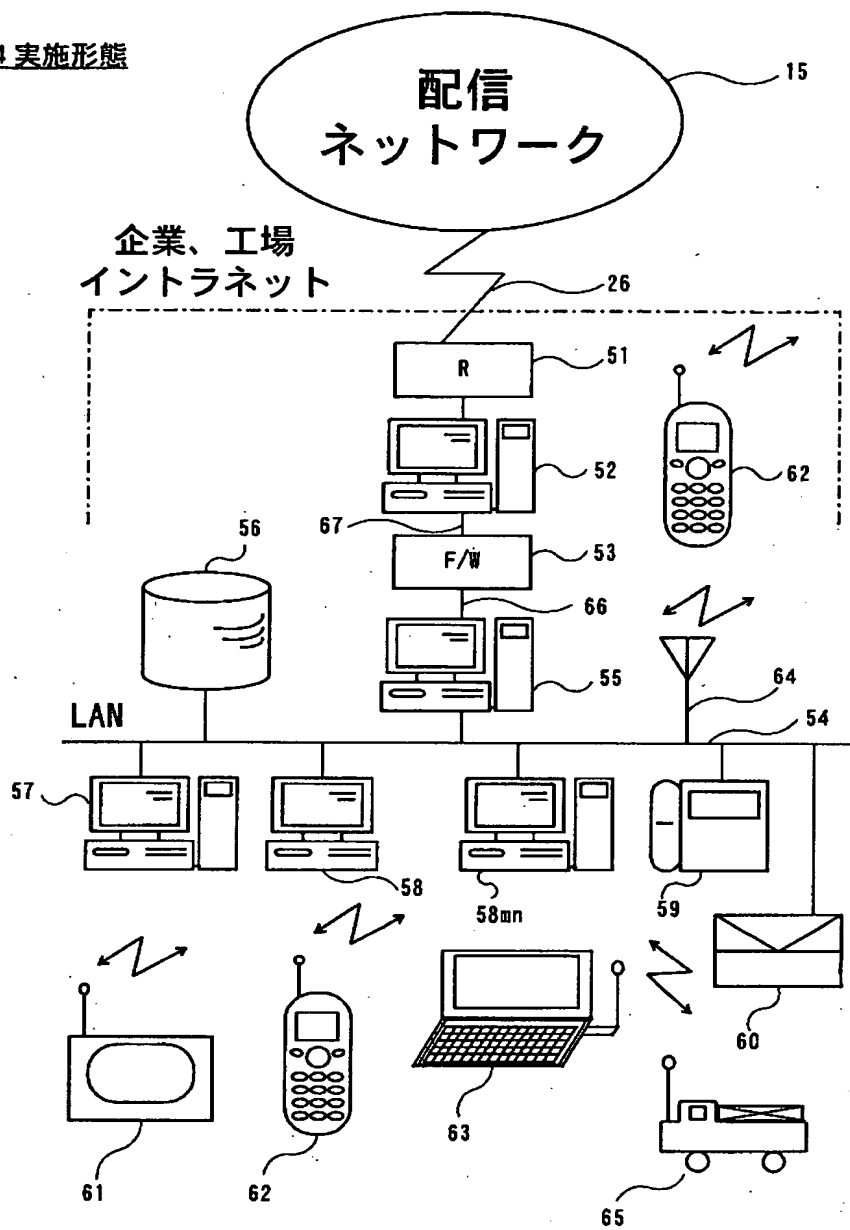


【図12】

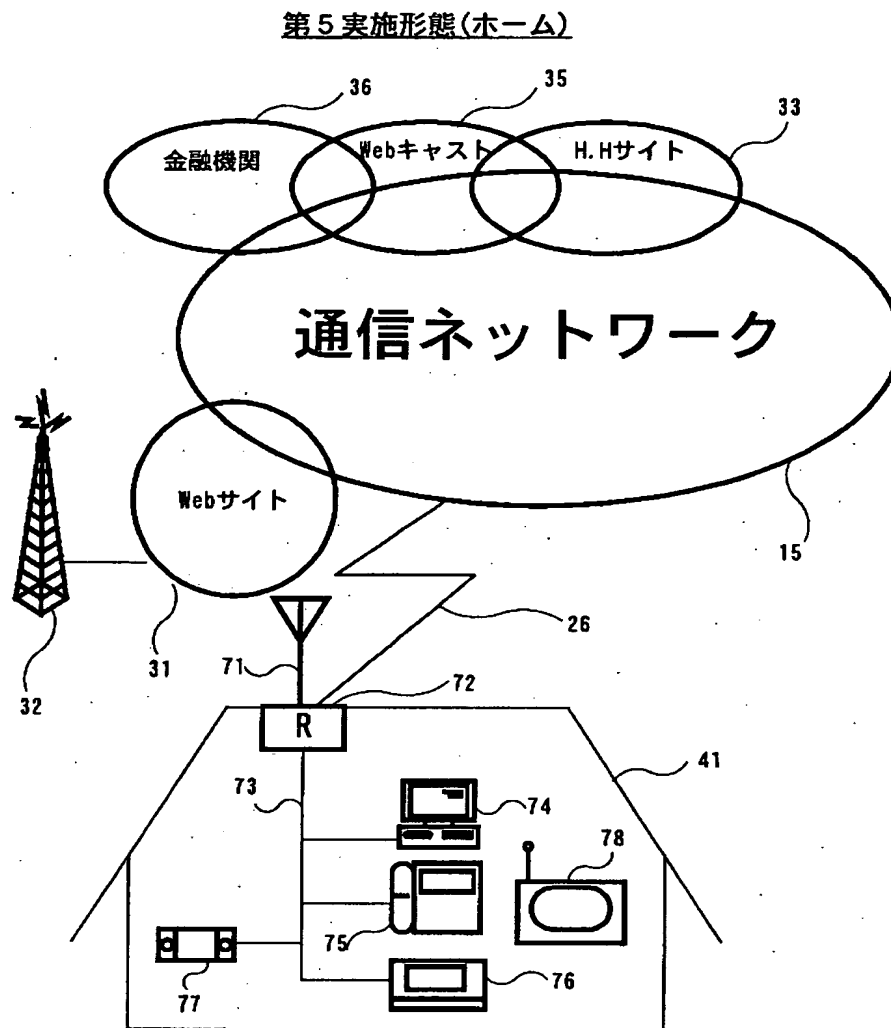


【図 13】

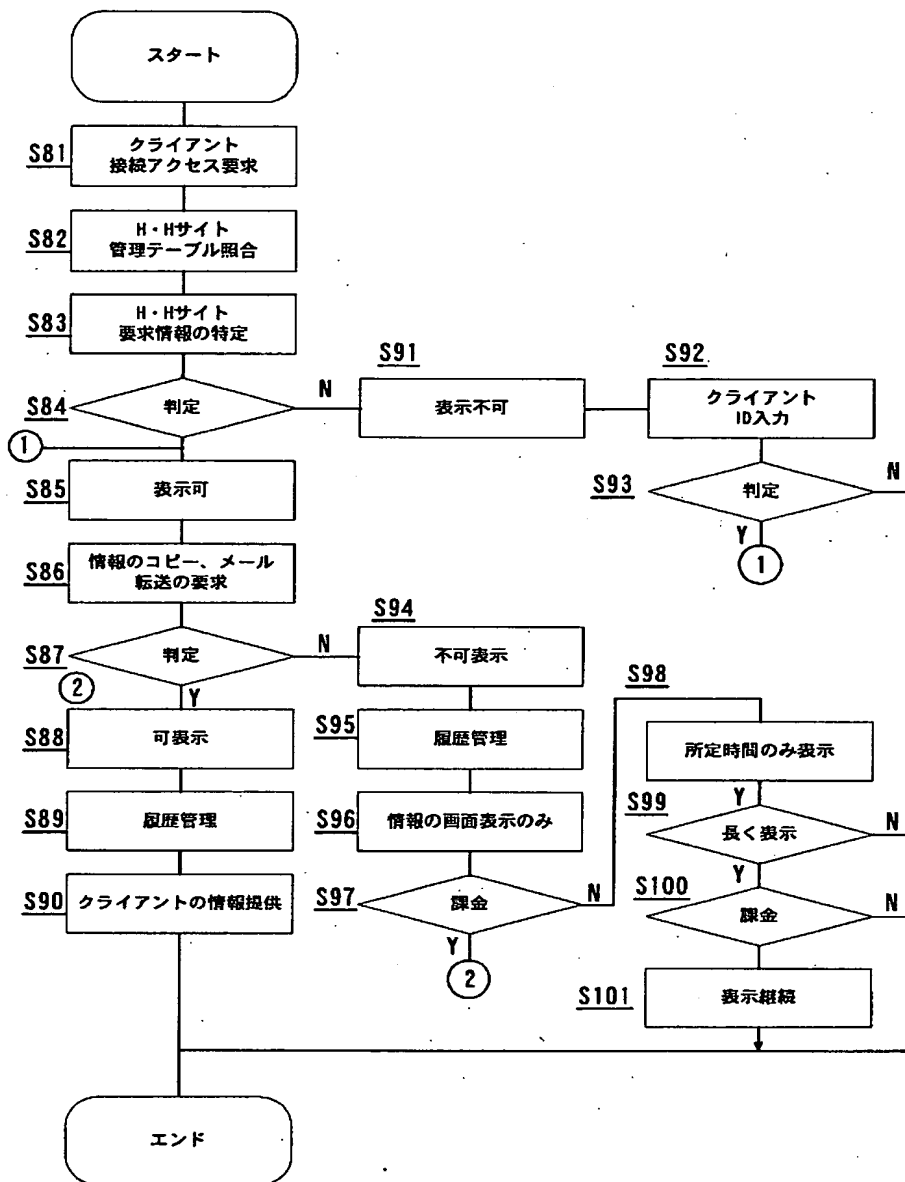
第4実施形態



【図 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 OSやプロセスを変更することなく、アクセス権限のないユーザに対するリソースの操作を制限し、しかも既存環境における禁止または制限事項を拡張すること。

【解決手段】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定し、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否するか、コンピュータリソースの内容に応じて課金する事によって許可する。

【選択図】 図2



出 願 人 履 歴 情 報

識別番号 [500083226]

1. 変更年月日	2000年 2月25日
[変更理由]	新規登録
住 所	東京都中央区月島1丁目2番13号
氏 名	ハミングヘッズ株式会社